

Balancing flexibility with risk

Do mobile technologies offer better business performance or a security hole?

Businesses often look to technology to fix a problem, when often all technology can do is amplify problems with existing processes and procedures. If a business has a problem, technology can make it bigger, happen faster and spread further. When businesses are based on sound principles and well run, the effect of technology is generally to enhance, streamline and improve. The two sides of the coin are particularly evident when extending access to internal IT systems outside the business premises. Wireless remote access opens the business up to new opportunities for efficiency and flexibility, but does it also increase the risks to the business, and if so, how can these be mitigated?

Contacts:

Rob Bamforth
Quocirca Ltd
Tel: +44 7802 175796
rob.bamforth@quocirca.com

Claire Kavanagh
T-Mobile UK Ltd
Tel : +44 1707 316474
claire.kavanagh@t-mobile.co.uk

RESEARCH NOTE:

The primary research data upon which this report is based was derived from an independent study conducted by Quocirca sponsored by T-Mobile. This involved 150 interviews of senior business and IT management from a broad cross section of industries in the UK. Respondents were divided evenly from among small (200-1,000 employees), medium (1,000-10,000) and large (10,000 and above) organisations. Other sources of data are highlighted where they are used.

We would like to thank T-Mobile and the interviewees who contributed their valuable time.

KEY FINDINGS

- **IT plays a vital role to many businesses, and most expect it to be constantly available**
Although almost one in five managers believe the importance of IT is often over rated, it has become the mainstay of the efficient running of most businesses. The need for IT services now spans beyond the traditional business hours of the working week, and over two thirds of UK businesses expect the IT applications to be available for 24 hours of every day of the week. This increases pressure on the IT function to have resilient systems, and is an indication of how suppliers, customers and employees need to have access outside office hours and therefore outside the office.
- **Security is seen as an IT problem, not a broader business issue**
Most companies rate security concerns as important reasons for limiting the number of employees who can work from home, or access IT services while travelling or out of the office. The ideas for wireless remote access often originate in the IT department, and here the knowledge of what attacks may be possible, fuelled by scare stories in the media increases the emphasis on protecting assets, and less on ensuring the continuity of business processes. Wireless remote access has broader business benefits, and these need to be taken into account alongside technical security issues.
- **Fears over personal security impact the numbers of employees given mobile or remote access**
While the security of data has a major affect on plans to deploying mobile solutions, there are significant concerns over personal security for two thirds of businesses. The risks are unlikely to come from a desire to attack the company, but from the intrinsic value of mobile devices and hardware, and the ease with which they can readily be disposed of if stolen. In addition to managing the disruption caused by theft and potential loss of confidential data or access rights, the business has to replace the missing item, and device costs are also a major concern.
- **Homeworking has many benefits, but its increased business resilience is not fully appreciated**
Working from home is seen as an important way to increase productivity, reduce staff turnover, and benefit the environment for over two thirds of businesses, but less than half see its effect on business resilience as valuable. The availability, performance and low cost of home broadband networks and widespread use of mobile phones has made working from home a viable and effective way to extend the organization and increase its flexibility.
- **Wireless remote access is seen to increase the resilience and flexibility of the business**
Despite the security challenges, wireless remote access makes a business more able to adapt to threats and changing conditions. Although a financial return on investment is important, over half of companies recognise the broader value proposition these technologies have on the agility of the organization and that their use can increase competitive advantage.

Introduction

The business processes of any organisation are affected by many external influences. Some are deliberate directed threats, some accidental damage or mistakes; others are just the knock on effects of reactions to market conditions.

Mostly these affect the business in a bad way, so they need to be prevented if possible, or their effects mitigated. However, others may open up opportunities, and those flexible enough to be able to react will have the potential to gain most benefit.

As organisations open and extend access to their IT services and applications, they increase their reliance on these services and increase areas of vulnerability. Many terms are used to describe the abilities of organisations to cope, but this report will use the term resilience to describe an organisation's resistance to threats, agility to embrace new opportunities and levels of security to offer continuity of services.

The report looks at impacts of wireless or remote access on the resilience of small, medium and large enterprises and how security balances against flexibility. It is intended to be read by those with responsibility for sourcing mobile technologies and dealing with mobile suppliers.

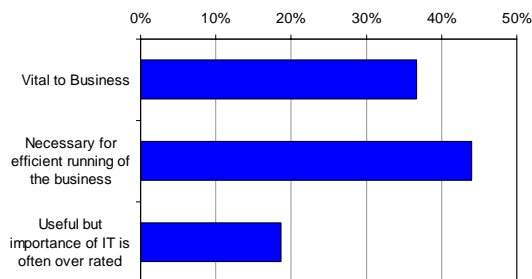
It offers them peer review and information for their discussions with vendors. As a background, 150 business and IT managers were interviewed from a mix of industries across the UK.

1 The importance of IT

At one time computer and communications technology played an add-on role in only the more technical aspects of many industries. Now it has spread to become fundamental to the operation of all businesses as information and its flow have become critical business assets (Figure 1).

Figure 1

What's your overall view of the role of IT?



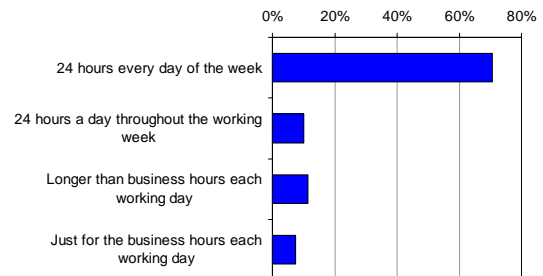
The business justification for IT and communications investment is generally to add value or reduce cost, but it can also be justified on risk reduction, especially if it adds to the resilience of the organisation.

IT and communications infrastructure plays a dual role in the resilience of any organisation. It is susceptible to failure, attack and mis-use, yet can provide flexibility, alternatives and efficiencies. In today's global economy, businesses rely

on their networks and IT services being available well beyond the local business working hours, as employees, customers, partners and suppliers need access anytime, anywhere (Figure 2).

Figure 2

What is the general expected availability of access to IT applications or services across the business?



Wireless and remote access to IT certainly exposes more points of vulnerability – open networks, new types of devices and usage in uncontrolled locations outside the corporate perimeter, make the task of security harder, but increase the flexibility of the business.

Sound business and technology strategies which tackle all the security issues are necessary to ensure that wireless and remote access plays a positive and effective role where the increased resilience it brings outweighs any new challenges.

However with suitable business and technology strategies in place, the security issues can be addressed, ensuring that wireless and remote access brings extra resilience to the business, outweighing any new challenges

2 The security challenge

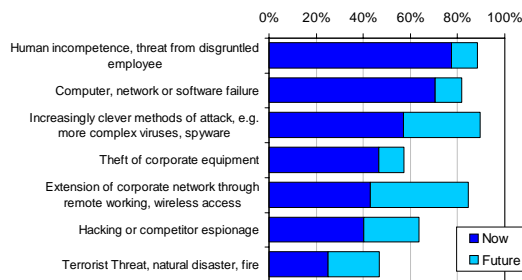
Security is often the first point of focus, and in any industry there is always a good deal of media comment, scare stories from those with agendas to sell or offer services, and fear of the unknown. This is not without some justification, but businesses must take a pragmatic view.

Total security is never achievable, and focussing on one over promoted or glamorous aspect of security can lead organisations to miss a more mundane threat. For example a company may spend thousands on redundant systems and networks, which are left idle when no one is allowed in the building due to bacteria in the air-conditioning.

A balanced view is required. Security is required to safeguard resources to ensure that business processes can carry on as normal. Whilst some items are made more safe and secure from theft by keeping them under lock, key and control, this may hamper the organisation's ability to respond to other challenges, ultimately undermining the security of the overall business (Figure 3).

Figure 3

What do you feel are the major causes of corporate data risk, now and in the future?



From "IT Security – Bridging the Gap" – Summer 2004

It is useful to look broadly at the threats and challenges that affect the resilience of a business, in order to identify how these should be dealt with in the business strategy. The introduction of new technologies, such as wireless or remote access can then be better assessed. Threats fall broadly into a 4 categories:

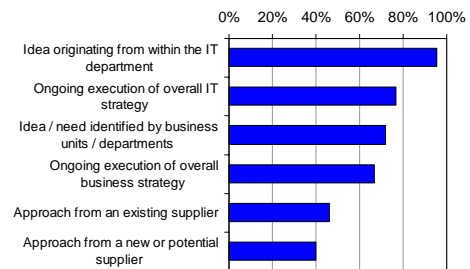
- Denial. IT is an important part of most businesses, and when a service or information access is not available, the business suffers. Security experts think of denial of service attacks on servers, but if access to the office is prevented by a tube strike, terrorist alert or burst water main, the business still has a problem. Extending access and services over open networks increases the susceptibility to attacks and network failure, but mitigates against other external problems.
- Revolution. Unexpected changes do not have to happen overnight, but when these are large, businesses have to adapt. The effects of a major shift in the market, natural catastrophes, transport chaos, new technology adoption in foreign markets can all be managed by short term security and risk management, but the longer term impact is generally greater, requiring re-organisation, relocation and changes in working practices. Those organisations with more highly mobile workforces can be more flexible with office location, desk space requirements and travel needs, and so adapt faster.
- Integrity. When information is lost or damaged, business processes are affected. It could be infected by a virus or compromised by a hacker, or through process errors, employee carelessness or wilful damage. Often the focus is on protecting from external threats, but there are many internal challenges, which can be addressed with policies and user education. Wireless or remote access increases the potential for external threats and system failures affecting information integrity, but if it replaces paperwork and overly bureaucratic workflows this can have a positive impact on data integrity.
- Confidentiality. Control of access to information is clearly important. Supplier transactions, patient records, payroll, secret recipes need to be kept from those who should not see them, but made as easily available as possible to those who need to gain access. This is a human process supported by technology. Passwords and encryption, just like locks and keys, only provide

security if used correctly and if overused, or over-complicated, can restrict legitimate access.

Security is too important to be solely a technical issue, and must be assessed alongside overall access to IT. Too often these issues are viewed from a purely technical direction, from where the ideas originate internally, when an external perspective might give a more balanced view of the risks against the overall value proposition (Figure 4).

Figure 4

Wireless Remote Access - Which of the following would you say are significant in prompting investments in these three areas? (i.e. creating ideas for new projects)



This requires a more strategic view to be taken of who needs to access what, where and when in order for the business to be flexible and resilient, whilst still protecting the assets of the organisation. Some need rigorous protection where physical security goes alongside IT security, for example certain data might only be accessible on site, but if security constraints are applied too tightly, the business processes they are intended to protect might be stifled.

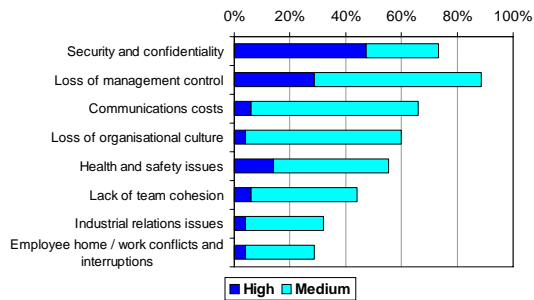
3 Risks in the home office

The number of employees needing to access and use IT outside the constraints of the office is significant and increasing. Even within the workplace, we have moved a long way from when IT was provided in a dedicated closed off room, and laptops, handheld devices and wireless networks are extending access beyond desks and fixed work stations to the location the employee needs – on the shop floor, in warehouses, meeting rooms, with customers and at home.

The use outside the office or organisational perimeter is where there is most concern. Employees who take work home and use wireless or remote access to connect back to the central IT systems need to be aware of their responsibility to manage the security risks. Network security issues can be addressed with appropriate technology, but well managed and communicated policies are necessary for those working from home to take the appropriate actions (Figure 5).

Figure 5

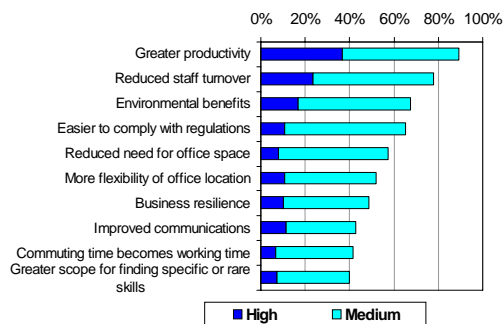
What are the main inhibitors for limiting the number of employees who are allowed to work from home?



The ability to work from home can be a real benefit to a company's resilience to external challenges, allowing employees to cope with travel disruption, temporary office closures and adverse weather. It can also be more relaxed, and while it is important to keep this benefit, those working from home, especially for extended periods should still be made to feel part of the team. This not only keeps up the level of professionalism, but also reinforces the responsibility that employees have to manage the security and confidentiality of business resources (Figure 6).

Figure 6

How important are these benefits for the business from home working?



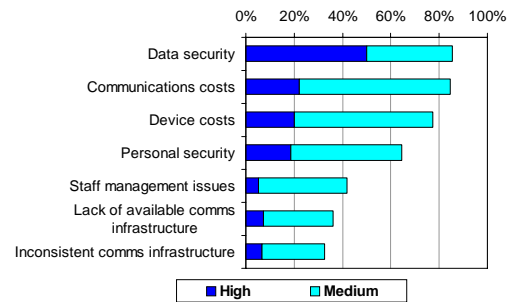
Many of these benefits are well documented, but the impact on business resilience is blunted by the perceived security risks. While these are real from the narrow technical and management perspective of securing the data, access and integrity, the positive impact on securing the continuity of business processes as a whole is often missed.

4 Risks in the "ad hoc office"

Working from more remote locations brings further challenges, and especially for security. Again the network access can easily be secured, but all too often users are careless. PIN numbers and passwords are often left unset, and the devices themselves are easily lost. These are difficult issues to address with technology, but far easier to address with strong policies which make users aware of their responsibilities (Figure 7).

Figure 7

What are the main inhibitors for giving more employees who travel widely nationally or internationally, mobile or remote access to IT?



Those who are travelling specifically to meet other companies - customers, suppliers or business partners - might gain access while on those companies' sites, either through wireless access, or through the company network. Visitor wireless LAN's or partner hotspots can provide a useful service which adds to the business relationship.

The extra flexibility this type of working brings to an organisation and the individual is very useful, giving employees access to the information necessary to do their job, and allowing them to make use of what might have been lost time.

It naturally extends to public places, and many laptop users can be seen working in coffee shops, hotel lobbies, airport lounges and car parks. This flexibility allows almost any location to become an ad hoc office, and companies with pressures on meeting rooms and office space, often create informal meeting spaces in public areas.

Despite the relaxed atmosphere, it is even more important that employees do not let their guard down. With well protected devices, loaded with the latest security software and virtual private network connections to their employers systems, the technology is secured, but again the user is the weakest link. Not only for how they keep the data and devices in their charge secure, but their personal security is also at risk.

Phones, PDAs and laptops are all potentially valuable targets for theft, even whilst being used. Employees should take extra care in public places by not drawing attention to valuable technology, and using unbranded carrying bags, or choosing those that do not solely appear to be for portable devices.

Whilst most theft is likely to be for the value of the device, data will be lost, even if not compromised, and so automated backup or data synchronisation is an important safeguard to protect as much as possible, and allow the user to start working again.

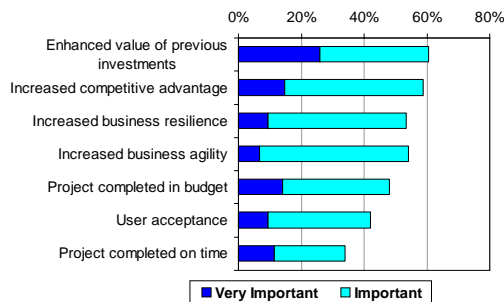
Further resilience can be achieved if mobile devices are fully synchronised to a central server, allowing a replacement device to be configured to be identical to the one lost, stolen or damaged. For smart handheld devices, a remote kill or wipe could also protect the data on the device from being compromised.

5 Conclusions

While many companies are looking for the best return on new investments, and how these add value to existing systems, a good deal of emphasis is being placed on the business's ability to react and respond rapidly to external market forces and threats (Figure 8).

Figure 8

How important are other factors beyond return on investment for a wireless remote access project?



Much effort is rightly placed on the ability of IT departments to recover after a disaster, with backup processes, redundant and fault tolerant systems. In the hopefully rare event that exercises these plans, their value is immediately recognised.

However, before the disastrous stage is reached, there are many crises whose effects can be mitigated. This is one area where wireless and remote access can play a part in spreading the functional operations over a wider domain to increase overall business resilience. There are points of vulnerability that need to be addressed with security solutions, education and above all, policies, but these do not need impede the flow of the business.

With security issues handled appropriately, wireless and remote access can have a positive effect on an organisation's flexibility and agility:

- Recovery. In the event of external events or internal failures, overall business processes can recover faster being de-centralised into multiple mobile locations.
- Responsiveness. Staff can be deployed rapidly in larger numbers to trouble spots to fix problems quickly.
- Isolation. Keep key individuals in the business process away from dangerous or problematic situations.
- Alternatives. Wireless and remote access provides alternative routes and channels for external communication increasing the flexibility of the business.

When viewed in isolation from the needs of the business, security fears can skew thinking into purely protecting assets, rather than protecting business processes. The overall risks need to be assessed, rather than just threats, and security issues are better dealt with as part of a broader business resilience function than elevated to a status of their own.

5.1 Acknowledgements

This kind of research is crucial to all of us in the business and IT community - suppliers and customer organisations alike. We would therefore like to thank all of those participants who contributed so generously, with patience and good humour, towards a better understanding of issues in this important area, and to the sponsor of the research behind it.

About T-Mobile

T-Mobile International is one of the world's leading companies in mobile communications. By Q3 of 2004, more than 109 million people were using the mobile communications services provided by companies in which T-Mobile or Deutsche Telekom have a majority or minority stake. And all that over a common technology platform based on GSM, the world's most successful digital wireless standard. This also makes T-Mobile the only mobile communications provider with a seamless transatlantic service.

T-Mobile UK, the fastest growing UK network, currently has 16.1 million customers. Its UK network covers over 99% of the UK population and currently offers roaming on 370 networks in 163 countries, including the USA. T-Mobile UK has 1,900 Wi-Fi locations, giving customers the largest UK Wi-Fi network as well as the largest network in Europe and the USA.

For more information about T-Mobile UK, please visit www.t-mobile.co.uk or contact the press office on +44 (0) 70171 50150.

If you have any further questions concerning this white paper please contact:

Claire Kavanagh

T-Mobile (UK) Ltd

Hatfield Business Park

Hatfield

Hertfordshire

AL10 9BW

e-mail: claire.kavanagh@t-mobile.co.uk



About Quocirca

Quocirca is a UK based perceptual research and analysis company with a focus on the European market for information technology and communications (ITC). Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry in the following key areas:

- Business Process Evolution and Enablement
- Enterprise Applications and Integration
- Communications, Collaboration and Mobility
- Infrastructure and IT Systems Management
- Utility Computing and Delivery of IT as a Service
- IT Delivery Channels and Practices
- IT Investment Activity, Behaviour and Planning

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help its customers improve their success rate.

Quocirca has a pro-active primary research programme, regularly polling users, purchasers and resellers of ITC products and services on the issues of the day. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Morgan Stanley, Oracle, Microsoft, IBM, CA and Cisco. Sponsorship of specific studies by such organisations allows much of Quocirca's research to be placed into the public domain. Quocirca's independent culture and the real-world experience of Quocirca's analysts, however, ensures that our research and analysis is always objective, accurate, actionable and challenging.

Most Quocirca research reports are available free of charge and may be requested from www.quocirca.com. To sign up to receive new reports automatically as and when they are published, please register at www.quocirca.com/report_signup.htm.

Contact:

Quocirca Ltd
Mountbatten House
Fairacres
Windsor
Berkshire
SL4 4LE
United Kingdom

Tel +44 1753 754 838
Email info@quocirca.com

The logo for Quocirca, featuring the word "quocirca" in a lowercase, sans-serif font. The letters "qu" are in blue, "o" is in red, "c" is in blue, "i" is in red, "r" is in blue, "c" is in red, and "a" is in blue.